Securing the Internet

Cyber security experts converge for Locked Shields exercise in Estonia

By *per Concordiam* Staff

Estonia's Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a powerful testament to NATO's goal of protecting the Internet. The 2007 cyber attack on Estonia revealed NATO vulnerabilities in cyber security, but also served as a catalyst for Estonia to become a world-renowned cyber defense nerve center.

In April 2013, 250 security professionals from nine European countries participated in the CCDCOE's annual Locked Shields cyber security exercise to measure how effectively the Alliance can fend off cyber attacks in an era of increasing malware sophistication. The two-day exercise replicated a real-life crisis to test the skills of cyber experts from Estonia, Finland, Lithuania, Germany, the Netherlands, Italy, Poland, Spain and Slovakia.

The fictional scenario featured the unstable nation of Boolea under attack by a strong insurgency openly assaulting coalition forces. At the same time, civilians were afflicted by a deadly epidemic. Response teams from organizations such as the United Nations and the Red Cross learned that their computer systems were under attack, crippling relief efforts. The aid organizations asked coalition forces for help to keep their systems running at 10 locations for two to three days.

To resolve Boolea's situation, computer experts from each participating country and NATO competed to develop the best defense. Collectively, they were known as the blue teams, or the defenders. The attackers were part of a red team of hackers enlisted to compromise the computer systems of the blue teams.

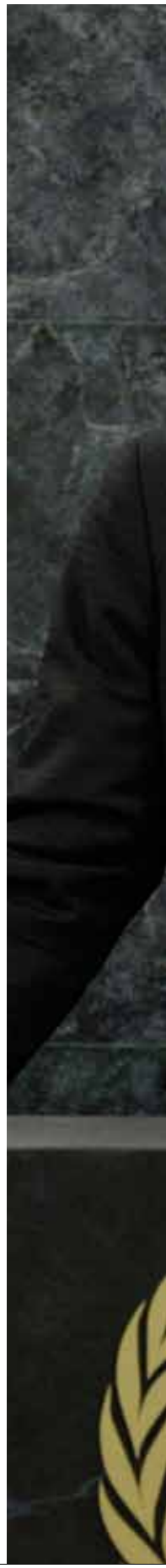
NATO emerged as the winner, with Estonia in second, but competition was fierce. "It is good to see that the blue teams have really prepared well for this year's exercise, and the opposing team had to work a lot harder to keep the difficulty level high for the defenders," said Jaan Prisalu, director general of the Estonian Information System's authority, according to the center's website. Aside from the technical aspects, working together in a practice scenario helped participants better understand different cultures, diverse ways people do things, and even different languages.

Estonia as cyber pioneer

Estonia has emerged strongly from the April 2007 cyber attack that overwhelmed the websites of banks, ministries, parliament and television stations. The country's latest development is the creation of an all-volunteer "cyber army" known as the Cyber Defense League. It empowers citizens to participate in national cyber security. The unit's 150 members are some of the country's best and brightest information technology minds. They would be among the first contacted should Estonia find itself under attack.

"We have slowly gotten to a point where we admit that cyber attacks and cyber wars are a major threat and not just child's play by misguided hacker-geeks. … When threats are no longer classic threats, our response can no longer be classic either," Estonian President Toomas Hendrik Ilves said at a cyber conference.

In 2012, for the third year in a row, Estonia was ranked by the nonprofit human rights organization Freedom House as having the most Internet freedom. Germany and the U.S. were second and third. Antivirus software vendor McAfee rated Estonia as one of the most prepared countries against cyber attacks.



Estonian President Toomas Hendrik Ilves speaks to the United Nations General Assembly about Internet security in September 2013.

GETTY IMAGES

"We have slowly gotten to a point where we admit that cyber attacks and cyber wars are a major threat and not just child's play by misguided hacker-geeks."

– Estonian President
TOOMAS HENDRIK ILVES

In 2012, the "Eurograbber" virus stole 36 million euros (about $47 million) from more than 30 European banks via cellphones.

A bank customer accesses his account through his mobile phone in June 2013 in Paris. The need for cyber security increases as more people use mobile phones for financial transactions.

AFP/GETTY IMAGES

In Ilves' view, the key to security online is identifying users. Estonia enlists a secure online identification system, and the government serves as guarantor of online transactions. Each citizen has a government identification card that protects digital signatures and personal information.

"We use a two-factor identification system in which the ID is protected by both a chip and a password. A binary key or public key infrastructure guarantees securely encrypted transfer of information," Ilves wrote in an article published in *The New York Times* in April 2013.

Estonians access their government and public services online, and vote in national elections via the Internet. In 2001, about a quarter of Estonians cast ballots online. Nearly all banking transactions take place online, and the number of online banking users exceeds the country's population. Ninety-five percent of tax returns and prescriptions are filled online.

Protecting mobile connections

As the Internet plays a larger role in most people's lives, protecting mobile connections has increased in importance. In 2012, the "Eurograbber" virus stole 36 million euros (about $47 million) from more than 30 European banks via cellphones. This malware was designed to defeat the two-factor authentication systems used by most banks — the safeguard of sending the customer a text message with a temporary password.

The infection starts with a click on a malicious link or the opening of spam email. At that time, the ominous Trojan infects the computer, unbeknownst to the user, and waits for the user to log into a bank account. The Eurograbber then intercepts the bank's website and displays a bogus page that asks the customer to complete a "security upgrade." The page requests the mobile phone number of the user and sends them a text.

"It's multi-staged, in that it focuses on the computer and the mobile device," Darrell Burkey, anti-virus expert at Check Point Software Technologies, noted in an article on the Bank Info Security website. "It's sophisticated in the way it goes about taking advantage of the two-factor authentication. It's targeted. It's stealthy. And unfortunately, it's successful."

CCDCOE's future

Since its establishment in 2008, the CCDCOE has heightened NATO cyber defense. The center's mission is to enhance cooperation, research and development and information sharing among nations on best practices. Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain and the U.S. are partners at the center. France, Turkey and the United Kingdom are slated for membership in 2014, and Iceland

PER CONCORDIAM ILLUSTRATION

announced in April 2013 its intent to join. In October 2013, Estonian and Finnish defense ministers agreed to allow Finland to contribute two experts to the center starting in 2014, even though the country is not a NATO member.

CCDCOE partnerships with various institutions such as the Cyber Defence Research Centre (CODE) of the Universität der Bundeswehr München, the NATO school, and the U.S. Naval War College are instrumental in its success. "It is definitely a win-win situation for both sides because we gain the most recent academic knowledge from a highly sophisticated research institute and CODE's students will benefit from a very skilled mentor whilst working on their theses, not to mention the experience and contacts made during this period," the CCDCOE noted in a news release.

Kenneth Geers, a U.S.-based cyber security expert who has worked at the CCDCOE, likened hackers to pirates who probe opponents for weaknesses to exploit. A solid defense forces cyber criminals to turn their attentions elsewhere. "You can't wait until a conflict erupts" to start building cyber defenses, Geers told an audience at the George C. Marshall European Center for Security Studies in July 2013.

The exercise's name, Locked Shields, refers to a method of defense on an ancient battlefield. If only one soldier is holding a shield, he is protected only on one side, Rain Ottis, a CCDCOE cyber security expert, explained in a video from the 2012 exercise. But several soldiers standing together with shields can protect each other's vulnerable sides. "If you have many men, locked shields can form an impenetrable wall. This is what we wanted to convey — this message that we have to work together. We have to lock our shields and protect each other."

Working together in programs through the CCDCOE in exercises such as Locked Shields strengthens those cyber defenses. "I firmly believe we owe the success of the exercise to our partners, without whom this event could not take place, and we are hoping to cooperate with all of them again for Locked Shields 2014," said Col. Artur Suzik, director of the CCDCOE. □